Reliable Data Transmission for Smart Substations

Based on Blockchain

Weilun Lao[1], Haoxin Wang[2*], Rui Zhang[2*]

[1]Guangzhou Power Supply Bureau, China Southern Power Grid Co. Ltd., Guangzhou, China
[2]State Key Laboratory of Information Security (SKLOIS), Institute of Information Engineering (IIE), Beijing, China

laoweilun@guangzhou.csg.cn
{wanghaoxin, r-zhang}@iie.ac.cn

Abstract. This paper investigates the important problem of ensuring reliable data transmission for smart substations. We give a first formal model including network assumptions and security requirements as well as a scheme based on blockchains and cryptographic techniques. Especially, we use the idea of network coding and blockchain to leverage the unstable transmission into a more stable one, trading reliability with redundancy (network bandwidth.) Finally, we apply both theoretical and experimental analysis. The result indicates that our solution is effective.

Keywords: smart substation; reliable communication; blockchain

1 Introduction

With the development of sensing / measurement technology, information communication technology (ICT), computer and control technology, substations entered a next stage, smart substation [1] [2] [3]. The smart substation was designed from the top level and set up on a unified information platform, namely the IEC 61850 standard, to implement status censoring, data acquisition, online monitoring, and state diagnose of the primary and secondary equipment.

1.1 Overview of Data Flow of Smart Substation

There is a unified server inside a smart substation, which collect panoramic data resources to realize high integration of information and real-time data exchange, and provid data analysis, data identification, data storage, data subscription, and other services. The server of the smart substation, together with a data center in the cloud, also realizes many advanced applications, such as automatic control, intelligent regulation, online analysis, decision-making, collaborative interaction, and utilizing multi-source information association analysis and artificial intelligence (AI) technology.

H. Wu et al. (Eds.): CSIEDE 2022, ACSR 103, pp. 639–646, 2022.
https://doi.org/10.2991/978-94-6463-108-1_71

There are two types of data sources. The data related to the primary equipment (such as transformers and generators) consist of grid analog quantities, state parameters, alarm signals of the primary equipment, and operation status and action signals of the secondary equipment. The data regarding the secondary equipment (aka. the low-voltage electrical device that monitors, controls and protects the operating state of the primary equipment) consist of status and real-time alarm information of subsystems for online monitoring inside stations, inspection robot, video surveillance, fire protection, security precautions, environment monitoring, SF6 monitoring, and lighting control. Online monitoring data include the operational state information of transformer, reactor, CT, CVT, coupling capacitance, arrester, circuit breaker, GIS, and the secondary equipment itself.

1.2 Related Work

The concept of smart substation emerged from smart grid [3] [5] and gradually become an important part of investment for smart grid. Though IEC 60870-5-104 was gradually replaced by IEC 61850, in many substations, old-generation equipment was not able to communicate with IEC 61850. Zhang et al. [6] reviewed the monitoring system in the smart substation, however, limited to Guangzhou area. They pointed out that cybersecurity concerns. On the other hand, it was widely-accepted that the security and reliability of data communication inside a substation or between a substation and a cloud data center are not quite covered by either IEC 61850 or 104 protocols. Therefore, the reliable and secure communication inside a substation, or between the control center to substations are of great concern.

1.3 Problem Setting

The IEC 61850 standard was developed under the need of smart substation [4], however, the experiment and the actual network configuration in many practical substations are star network. The centralized nature is control-oriented, and not much connection-oriented, though IEC 61850 is actually built upon TCP/IP protocols. In other words, reliable data transmission and sharing seemed not to be the main target of IEC 61850. Figure 1 shows the network and communication scenarios for a smart substation.

The first one is the communication from a device to another device via the server inside a substation, which is also known as internal information flow. In particular, a sensor captures some change in the status and transmits the signal to the substation server. The server then makes an immediate decision after certain computation, e.g., a auto reclosing of relay protection. The second one is a communication directly between two devices but not via any other device. Though this is quite typical in a 5G communication for a carrier network, typical communication scenario between a smart meter and an inspection robot roaming in the substation was recently proposed and implemented. The third one is remoting sensing, monitoring, and data mining. Raw data are acquired from the primary/secondary devices, and aggregated by the substation server at the edge side and turn into up-flow data which go to the data center in the cloud finally.

To summarize, data are transmitted and shared among the data center in the cloud side, the substation server at the edge side and the various devices inside a substation.

1.4 Our Contribution

In this paper, we study the problem how to achieve reliable data transmission and sharing among these entities are of great concern. Our treatment is three-fold: First, we give a system model. Based on the de facto. Standard IEC 61850, we abstract the communication model of different scenarios, such as inter-devices, device-substation server, data center-substation. We then formally define security requirements. Second, we give a scheme based on cryptographic techniques based on blockchains with security analysis. Finally, we give some experiment results, which indicates our scheme is effective.

2 Preliminary

2.1 All-or-Nothing Transforms (AONT)

An AONT [10] is a probabilitstic polynomial-time fucntion $T:\{0,1\}^k \to \{0,1\}^u \times \{0,1\}^v$ satisfying the following requirements: **a)** There exists a polynomial machine I such that $\forall\, x \in \{0,1\}^k$, and $\forall (y,z) \in T(x)$, we have $I(y,b) = x$. **b)** We call T is l-ANOT if any $x_0, x_1 \in \{0,1\}^k$, we have $\langle x_0, x_1, [T(x_0)]_{\bar{L}} \rangle \approx \langle x_0, x_1, [T(x_1)]_{\bar{L}} \rangle$ for any $L \in \begin{Bmatrix} u \\ l \end{Bmatrix}$, which inflicts random variables in $\left\{ [T(x)]_{\bar{L}} \,\middle|\, x \in \{0,1\}^k \right\}$ are indistinguishable from each other. If $T(x) = (y,z)$, we call define y the secret part and z the public part.

2.2 Digital Signature

A digital signature (DS) scheme [11] consists of three algorithms $(Gen, Sign, Verify)$: $(vk, sk) \leftarrow Gen(1^\lambda)$. The probabilistic algorithm takes a security parameter as input, and outputs a verification key vk and a signing key sk. $\sigma \leftarrow Sign(sk, m)$. The probabilistic algorithm takes a signing key sk and a message m as input, and outputs a signature σ. $1/0 \leftarrow Verify(vk, m, \sigma)$. The deterministic algorithm takes a verification key vk, a message m, a signature σ as input, and outputs 1 if the signature is valid. Otherwise, it outputs 0.

We say a digital signature scheme is existentially unforgeable against chosen message attack (EU-CMA) if for all probabilistic polynomial-time (PPT) adversary B, there exists a negligible function $negl$ to forge a valid signature after B has made polynomially-bounded q_s queries in any polynomial time t.

2.3 Blockchain Basics

Rooted from Bitcoin [12], a blockchain is a series of data blocks, called ledger, ordered by time, and jointly maintained by a number of servers, called nodes. The nodes that can write/read the ledger are sometimes called the miners, and the nodes that cannot write but only are called light-weight nodes. The mechanism that a miner is selected is called consensus. In a broader sense, a blockchain refers to the way that data/operations are organized. It has been renowned that it has implemented many advanced technologies such as cryptocurrency and smart-contract, and will reshape human society. There are two categories of blockchains: If any node can enter the network and have the chance to be the miner, it is called a permissionless blockchain, otherwise a permissioned one.

3 System Model

3.1 System Players

There are 5 types of entities in our system as shown in 0*A cloud server*, which include the control center and data center, In particular, we assume a full-fledged blockchain network is running and can exchange messages with the cloud server, or equivalently speaking, the blockchain network is a platform-as-a-service inside the cloud. *An edge server*, which includes the central information flatform inside a smart substation. *A blockchain terminal node*, which is a light-weight node, which can connect to the edge server and communicate with the blockchain network. *A blockchain network*, located in the cloud, which is able to verify any queried data from its ledger. *Devices* are those primary and secondary equipment inside a smart station, which samples signals and submits to the edge server.

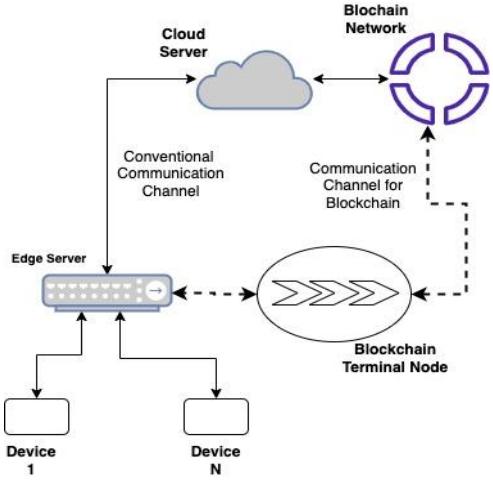

Fig. 1. Cloud-Smart Substation Communication with blockchain

3.2 Network Model

We assume the following network: The communication channel between devices and the edge server is stable but may suffer from eavesdroppers. The channel between edge server and the cloud server is stable for most of the time but sometimes may fail due to attacks, and so it is with the channel between the blockchain terminal and the blockchain network, but these two channels will not fail simultaneously. Finally, we assume the link between the cloud server and the blockchain network is reliable and private.

3.3 Security Model

We elaborate the security model from two aspects of view.

1) Security Goal

Our security goal is divided into two categories:

Confidentiality. Namely, the communication should private to any outsider, including the adversary or relay nodes in the communication.

Communication Reliability. Namely, a sender sends out a message, then it will eventually reach the targeted receiver.

2) Attacker Resource

An adversary may want to disturb the communication, and try to make the data transmission fail. Also, an adversary will try to know what is beyond its privilege.

Definition 1 (Confidentiality) If an adversary is not the intended receiver, it should not distinguish a transmitted message m from a random message m', where |m|=|m'|.

Definition 2 (Reliable Communication) Any message will finally reach its targeted receiver.

4 The Proposed Scheme

Before we give the detailed scheme, we briefly introduce the intuition behind the construction. We notice that according to our analysis and assumptions of the network model, only individual channel between the substation and the cloud can be unstable, i.e., there is at least one stable the channel between the cloud and the substation. Then we may use a technique similar to network coding [13]. Our scheme is depicted as flows:

4.1 Path Selection

Any message from the substation to the cloud or vice versa will be preprocessed and sent via both the traditional channel and blockchain channel. Any message sent inside the cloud or inside the substation will be sent via the actually link, namely, unnecessary to be transformed and sent multiple times. For simplicity, we don't discuss the latter case.

4.2 Message Preprocessing

First, assign a nonce **N** to a transmitted message **m**, first apply **m** to PRF, to acquire randomness for later use. then an ANOT is applied to **m**, with output c and r, where **c** is the public part and **r** is the secret part. Denote their signatures as **Sc** and **Sr**.

4.3 Message transmission

<**N**, **c**, **Sc**> is sent via traditional channel, while <**N**, **r**, **Sr**> is sent via the blockchain channel. For traditional channel, there is application layer security protocols like TLS. For blockchain channel, use ECIES or similar encryption algorithm (SM2) that are quite often available from practical implementations.

4.4 Message Reconstruction and Verification

To reconstruct a message, first search for the nonce **N**. Suppose there is a tuple <**N**, **r**, **Sr**, **c**, **Sc**> then verify if **Sc** is a correct signature for **c**, and **Sc** is a correct signature for **c**. If so, use the reconstruction algorithm of AONT with input **m**.

5 Analysis and Performances

5.1 Security Analysis

We briefly discuss why our scheme meet both confidentiality and communication reliability. By assumption, PRF always outputs good randomness.

For confidentiality, it is easy to see that since a message **m** is first transformed into two parts, and sent via two independent channels, also without any part, any PPT adversary cannot gain negligible information regarding **m** by definition of AONT. Second, the secret part **r** is protected by encryption algorithm in a blockchain. So any intermediate node will not be able to see both **c** and **r**, therefore, confidentiality is achieved.

For reliable communication, it is first noticed that the channels don't drop messages, namely, any message sent on the channel, though it can be delayed, but eventually reach the other side. Hence, due to the double guarantee of AONT, a message can be reconstructed, given enough time.

Combining the above discussion, we can then verify that our scheme meets message confidentiality and reliable communication simultaneously.

5.2 Performance Evaluation

We also implement our scheme with simulated networks and communications. We use a MacBook Pro with an Intel Core i9-9880H CPU@2.30GHz and 32 GB 2667 MHz DDR4, running macOS 11.5 (Big Sur) to perform the cloud server, and a Raspberry Pi 3 model A+ with Paspberry Pi OS Lie (32-bit) to serve the blockchain terminal, with runs HyperLedge Fabric client with Node.js preinstalled hence crypto-APIs such as ECIES/SHA1/ECDSA are supported.

Table 1. Overhead Caused by the Scheme

Operations	*Size of Data*	*Time(ms)*
AONT transform	512kB	1.38
AONT Reconstruction	512KB	2.47
ECDSA Signature Generation	512KB	13.38
ECDSA Signature Verification	512KB	18.51
Data Transmission Delay	512KB	3.85
Additional Bandwidth (Blockchain)	2.88MB	--

The number varies when data size varies. Network delay is only hopothosis.

From the simulation result, one can see that our scheme only add marginal cost to the system, and we conclude that our scheme is effective and useful.

6 Conclusion

In this paper, we investigate the problem of reliable data transmission regarding smart substations. We give a first formal model including network assumptions and security requirements as well as a scheme based on blockchains and cryptographic techniques. Especially, we use the idea of network coding and blockchain to leverage the unstable transmission into a more stable one, trading reliability with redundancy (network bandwidth.) Finally, we apply both theoretical and experimental analysis. The result indicates that our solution is effective.

Acknowledgment

The authors would like to thank the anonymous reviewers for valuable comments. The work is partially supported by National Natural Science Foundation of China (Grant No. 62172411).

References

1. Y. Song, J. Li, Analysis of the life cycle cost and intelligent investment benefit of smart substation, in: IEEE PES Innovative Smart Grid Technologies, 21–24 May 2012, Tianjin, 2012, pp. 7–11.
2. J. Chen, C. Huang, Z. Zeng, S. Qu, J. Luo, Q. Qin, “Smart grid oriented smart substation characteristics analysis”, IEEE PES Innovative Smart Grid Technologies, 21–24 May 2012, Tianjin, 2012, pp. 1–4.
3. B. Qi, Y. Yuan, Y. Yang, Q. Bu, J. Chen, “Chapter 1 - Overview of Smart Substations”, Editor(s): Y. Yuan, Y. Yang, IEC 61850-Based Smart Substations, Academic Press, 2019, Pages 1-24.

4. S. Kumar, N. Das and S. Islam, “Performance analysis of substation automation systems architecture based on IEC 61850”, *2014 Australasian Universities Power Engineering Conference (AUPEC)*, 2014, pp. 1-6
5. B. Sun, W. Sui and H. Li, "Applied research of supervision and control system in 110kV smart substation based on three layers of three networks," *2015 IEEE International Conference on Information and Automation*, 2015, pp. 896-900
6. M. Zhang *et al*., "Development of the Monitoring System in the Smart Distribution Substation in Guangzhou, China," *2020 International Conference on Wireless Communications and Smart Grid (ICWCSG)*, 2020, pp. 159-162
7. P. Jafary, S. Repo and H. Koivisto, "Secure communication of smart metering data in the smart grid secondary substation," *2015 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA)*, 2015, pp. 1-6
8. P. P. Parikh, T. S. Sidhu and A. Shami, "A Comprehensive Investigation of Wireless LAN for IEC 61850–Based Smart Distribution Substation Applications," in *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1466-1476
9. J. J. Claveria and A. Kalam, "Communication and Information Security Assessment of a Digital Substation," *2020 Australasian Universities Power Engineering Conference (AUPEC)*, 2020, pp. 1-7.
10. R. L. Rivest, “All-or-nothing encryption and the package transform,” in *International Workshop on Fast Software Encryption*, 1997, pp. 210–218.
11. S. Goldwasser, S. Micali, and R. L. Rivest, “A digital signature scheme secure against adaptive chosen-message attacks,” *SIAM J. Comput.*, vol. 17, no. 2, pp. 281–308, 1988
12. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, whit paper, 2011
13. Ahlswede R, Cai N, Li S-Y R, Yeung R W. Network information flow. IEEE Transactions on Information Theory, 2000, 46(4): 1204–1216